Expertise
and insight
for the future

Harry Naukkarinen

Ethernet Technology in Safety Automation

Metropolia University of Applied Sciences

Bachelor of Engineering

Automation Technology

Bachelor's Thesis

6 April 2020

Author	Harry Naukkarinen
Title	Ethernet Technology in Safety Automation
Number of Pages	44 pages
Date	6 April 2020
Degree	Bachelor of Engineering
Degree Programme	Automation Technology
Professional Major	
Instructors	Aki Raitanen, ICT Designer Kristian Junno, Senior Lecturer

Many companies have moved towards network protocols in automation, but some are still doubtful. The purpose of this thesis work was to study the current opportunities of using safety automation with Ethernet-based protocols for Mission Critical Networks team of AFRY Finland Oy.

The aim of the study was to discover benefits and restrictions of using Industrial Ethernet protocols instead of traditional serial-based protocols in safety automation. Another main issue in this work are factors to consider in collaboration between network and automation designers.

This work starts with a theoretical background of networks, and then moves towards Industrial Ethernet and automation. New technologies are also covered, and whether they are ready for safety related applications or not is clarified. The last chapter before closure considers Ethernet-based safety protocols, for example how to deal with redundancy of networks.

Conclusion for this thesis study is that using Ethernet-based fieldbuses brings advantages in modification and integration of automation systems, including safety functions. Additionally, Ethernet technology eases maintenance operations and other diagnostics. From network designing aspect, main concern was the redundant network. There are two types of redundancy, and a variety of protocols where to choose from. Choosing the right protocol depends on the response time and topology used. Time critical safety functions need faster response time for proper recovery. The objectives of this work were successfully gathered from documents by the manufacturers, electronic sources, and from other literature.

Keywords	Safety automation, Profisafe, Industrial Ethernet, Ethernet, Integration, Networks, Redundancy

Tekijä Otsikko Sivumäärä Aika	Harry Naukkarinen Ethernet Technology in Safety Automation 44 sivua 6.4.2020
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	Automaatiotekniikka
Ammatillinen pääaine	
Ohjaajat	ICT-suunnittelija Aki Raitanen lehtori Kristian Junno

Moni yritys on siirtynyt käyttämään tietoliikenneprotokollia automaatiojärjestelmissä, mutta silti osalla on vielä epäilyksiä niiden suhteen. Tämän työn tarkoituksena oli tutkia, millaisia mahdollisuuksia verkkopohjaisilla kenttäväylillä on turva-automaation näkökulmasta tällä hetkellä. Opinnäytetyö toteutettiin yhteistyössä AFRY Finland Oy:n Mission Critical Networks teamin kanssa.

Tämän opinnäytetyön tavoitteena oli ottaa selvää, millaisia hyötyjä verkkoteknologialla voidaan saavuttaa turva-automaatiossa, sekä millaisia rajoituksia verkkoteknologia tuo mukanaan. Toinen keskeinen käsite työssä oli automaation ja tietoverkkojen integraatio, josta tärkeimpänä yhteistyö automaatio- ja verkkosuunnittelijoiden välillä.

Tämä työ alkaa teoriaosuudella, jossa käsitellään ensin tietoverkkojen keskeisimmät asiat. Tietoverkkojen jälkeen siirrytään teollisuuden verkkoihin sekä automaatioon. Lisäksi työssä käsitellään yleistyviä uusia teknologioita, jotka voivat heikentää turva-automaation luotettavuutta. Kappaleessa ennen johtopäätelmiä käydään tarkemmin läpi ajatuksia verkkopohjaista turva-automaatioprotokollista, kuten esimerkiksi kahdennukseen vaikuttavista tekijöistä.

Työn tuloksena voidaan todeta, että verkkopohjaisten turva-automaatioprotokollien hyödyt näkyvät etenkin automaatiojärjestelmien muutoksissa ja integraatiossa. Tämän lisäksi laitteiston huoltotoimenpiteet ja diagnostiikka helpottuvat Ethernet-teknologian avulla. Tietoverkkojen näkökulmasta pääaiheena oli verkon kahdennus. Kahdennuksesta selvisi se, että kahdennusprotokollia on monia. Topologiat ja reagointiaika virheen sattuessa vaihtelevat protokollissa. Käytetty protokolla tulisi siis valita vaaditun topologian ja viiveen perusteella. Työn tavoitteena olevat tiedot saatiin hankittua valmistajien dokumenteista, verkkolähteistä, sekä muusta kirjallisuudesta.

Avainsanat	Turva-automaatio, Profisafe, Teollisuus-Ethernet, Ethernet, Integraatio, Tietoverkot, Kahdennus

Contents

List of Abbreviations

5G	Fifth Generation of cellular technology
ATEX	Atmospheres Explosible
CIP	Common Industrial Protocol
DCS	Distributed Control System
DMZ	Demilitarized Zone
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IRT	Isochronous Real Time
ISO	International Organization for Standardization
IT	Information Technology
MAC	Media Access Control
MES	Manufacturing Execution System
MM	Multi-mode fiber
NRT	Non-Real Time
OSI	Open Systems Interconnection
OT	Operational Technology

PLC	Programmable Logic Controller
RJ	Registered Jack
RT	Real Time
SD	Safety Domain
SIL	Safety Integrity Level
SM	Single-mode fiber
STP	Spanning Tree Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TSN	Time Sensitive Network
VPN	Virtual Private Network

1 Introduction

Ethernet technology has been used by consumers for a long time, but it had some major issues concerning the demands of industrial applications. Regardless of these issues, it has been modified to meet even the strict requirements of industrial safety applications, and it has become more common over time. For this reason, this study about Ethernet technology in safety automation was carried out.

The main purpose of this thesis work was to study safety automation and Industrial Ethernet in general, but also to find current solutions for using Industrial Ethernet protocols in safety automation applications. The aim of this work was to figure out what to take into consideration when designing Ethernet-based safety systems. The subject was mainly viewed by designing aspect, including network and automation technology. This thesis was carried out for Mission Critical Networks team of AFRY Finland Oy. AFRY is an engineering and consulting company, which was merged in 2019 from two companies named ÅF and Pöyry.

Thesis starts with theoretical background of networks, and then moves towards industrial Ethernet and automation. After background, this thesis provides an insight about how to consider between the Ethernet based safety protocols available. Proper protocol depends on the requirements of the application. Requirements include compatibility between vendors and what testing should be done to fulfill the demands. Reliable system is the main priority in safety related systems, which is why redundant network is one of the key points in this thesis. The necessity and profitability of safety automation over industrial Ethernet are also covered in this work.

2 Networks

2.1 Open Systems Interconnection Reference Model

Networks are used for sharing information between devices. For example, connecting computers to a network allows user to install software to several computers with one installation media. This makes the installation more time-efficient and usually cheaper

than using separate installation media for every computer. This is just one example of many practical uses to illustrate usage of networks.

Open Systems interconnection (OSI) reference model is a tool for demonstrating different steps behind sending packets through networks. OSI model is a stack, which consists of seven layers. OSI model is made for perceiving the functionality of networks. OSI model is not practical reference model, meaning that technically networks today do not have as many layers, but the logic of networks is easier to understand when cut into smaller pieces. OSI Model is created by International Organization for Standardization (ISO), which is a company that produce international standards. Standards are made to prevent disagreements between different manufacturers, but they are not mandatory. [1,20-21.]

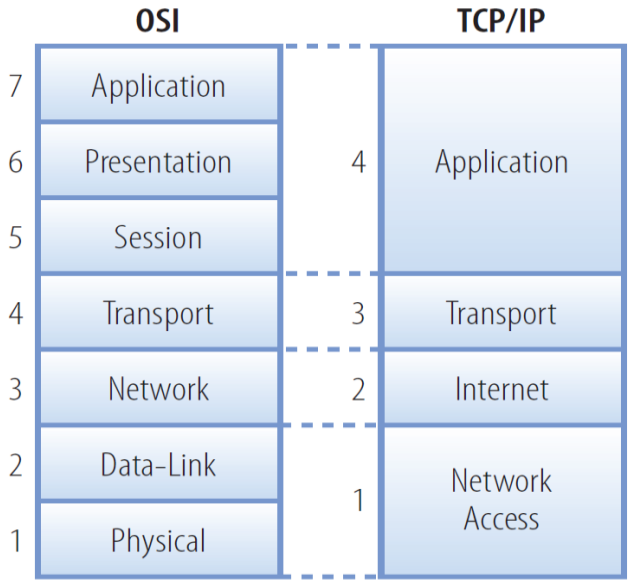

Figure 1 Comparison of OSI and TCP/IP Reference Models [1,44].

As figure 1 illustrates, layers in OSI model are ordered by physicality, the most physical protocols are at the bottom of the stack and more logical protocols are at the top. As shown in figure 1, there is also another model called Transmission Control Protocol/Internet Protocol (TCP/IP) model, which is more practical model. In this work OSI model is used as a reference model.

Application layer is closest layer to the end-user in OSI model, which is responsible for user interface. The received data from applications is modified into a form which people understand. This applies vice versa, human language can be translated for presentation layer. One of the most common practical use for application layer is email. [1, 23-24.]

Presentation layer has the responsibility to translate messages sent from device into a proper form for network devices. Without translation, the data cannot be forwarded via network. This layer also takes care of encryption and decryption of data for security reasons, encrypted data can be converted to original form by authorized receiver. Presentation layer uses a key value to identify the correct sender and receiver. [1, 24-26.]

Session layer determines connection between sender and receiver. This layer has authority to decide whether the connection is secure or not, but also if the participants are correct. If there are no conflicts concerning the participants, session layer keeps up the session and otherwise it will be ended. [1, 26.]

Transport layer ensures the correct transmission of data, which is re-sent if it is not correctly delivered. When transport layer gets data from upper layer, the data is cut into smaller pieces and it is brought back to the original form when destination is reached. For fluent delivery of message, transport layer utilizes port numbers. Receiver usually uses default port, which in most cases is 80. Port number can be modified for preventing excessive traffic in special cases. [1, 26-30.]

Network layer is responsible for hopping over different networks and optimizing the length of transmission between devices. Network layer equipment is aware of the Internet Protocol (IP) address of specific device. Packets of network layer consists of IP address and frames from data link layer. Although network layer equipment transfers frames, they do not care about their content. Network layer devices only look for the Media Access Control (MAC) address of the data link layer device and forwards information from there to transport layer and vice versa. [1, 30-31.]

Data link layer must define what to do with received frames. Frame consists of the content of data sent, and it also includes the MAC addresses. MAC address is a unique address of device, which is set by the manufacturer. Data link layer equipment is aware

of MAC addresses of devices but not of IP addresses. Data link layer translates logical address to physical address and vice versa. [1, 31-33.]

Physical layer covers the electrical signal between devices, which is received or transmitted via cable or radio waves. Physical layer defines the direction and amount of data flow, and if the hardware is capable of simultaneously receive and transmit data. Physical topologies are also one main aspects of physical layer, which determine the layout of devices, topologies are covered in this work later. [1, 33.]

2.2 Definition of Ethernet

Before defining Ethernet, it is important to know the main difference between Local Area Network (LAN) and Wide Area Network (WAN). LAN is mainly used to connect nodes in a small physical area, whereas WAN is mostly used in larger areas, and it connects Local Area Networks to each other. One practical example of Wide Area Network is the internet, where Local Area Networks are the home networks. [2, 19-20.] Advantages of LAN is the higher speed, and it is not as complex as WAN, which makes LAN also cheaper solution. Regardless of cheaper price, LAN is more restricted in distances, hardware and software options compared to WAN. [1,9-10.]

Ethernet is a protocol that is usually used in LAN environment. Ethernet can be found on the physical layers of OSI model. It describes the technology used for connecting devices in LAN, including hardware and cabling. [1,32.] It is important to standardize the technology used to reduce the compatibility issues between devices. Cable used in Ethernet depends on the application, where the main factors are speed, transmission length and price of the cable. Twisted pair cable is usually used in short distance transmission, and optical fiber in longer distances. [1,9].

2.3 IP Addressing

When designing Industrial Ethernet, it is important to have a vision of how the logical part of network is operating. IP address can be compared to a street address, a packet is routed in networks based on IP address. IP address consists of octets, which holds a value between 0 and 255. Octets are separated by dots and categorized in network

portion and host portion by subnet mask depending on the class of IP address. There are two IP addresses for default gateway, one is seen by the local users and other is for the users outside the local network. An example of IP address is 192.168.1.1. [2, 49-51.]

2.3.1 Subnet Mask

As mentioned above, IP address is divided into network portion and host portion, network masks main task is to determine this partition. IP addresses has different classes, which determines the quantity of nodes that is possible to connect to the network. [2,56.]

Table 1 Classful IP Addressing [2, 51].

Class	8 Bits	8 Bits	8 Bits	8 Bits
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host
Class D	Multicast			
Class E	Research			

As shown in Table 1, classes are alphabetically ordered starting by the longest host id, which means it can hold more nodes than other classes. That said, class a is meant for larger networks. Three most common classes are A, B and C, and they already have default masks defined. As in IP address, default mask holds two values of 0 and 255, 0 for host id and 255 for network id. Values are separated by points, for example class C mask is 255.255.255.0 and it is common for home networks. [2, 51.] Detail about addresses can be seen for example in command prompt in Windows 10 with ipconfig command.

2.3.2 Subnetting

Subnetting is used for splitting the network into smaller logical networks. This is important for efficient performance and higher security of the network. Subnetting is usually done by router, which is a network layer device in OSI model. For example, every floor on a building could have its own subnet. Subnet mask must be designated for the subnet. [2, 55-56.]

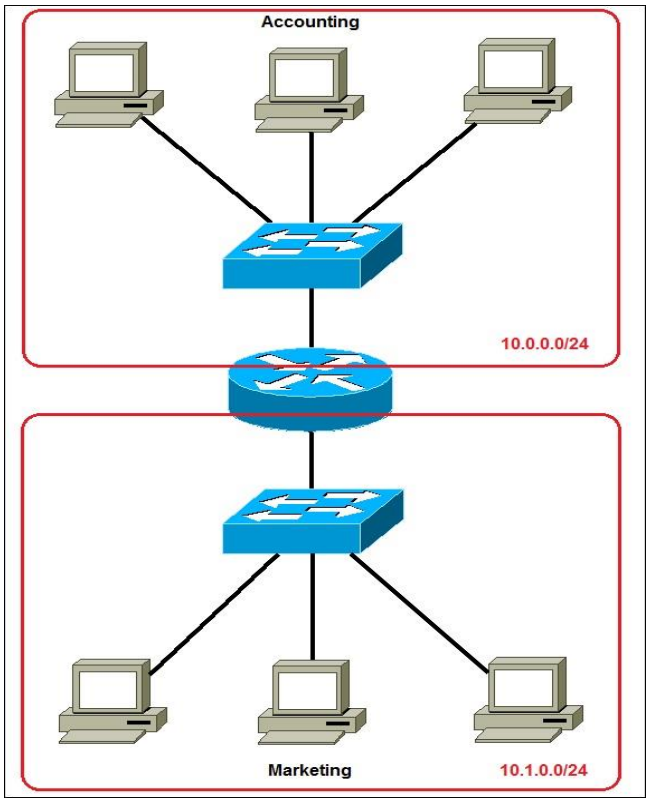

Figure 2 Subnetting example [3].

As illustrated in figure 2, by subnetting it is possible to divide different sectors in organization to their own smaller networks. This is used mainly for keeping crucial networks secure. For example, usually organizations do not want their industrial communication to mix with their office environment.

2.4 Network Hardware

Network hardware is used for physically and logically connect devices in a network. To optimize the functionality of network, hardware should always be suitable for the environment it is going to be used. Hardware designing is also crucial for the operation of network. Equipment should be installed in such a manner it is meant to be used for ensuring optimal functioning of the network. [1, 201.]

Repeater works like an amplifier, incoming signal gets strengthen by repeater, as a result, the outcoming signal is stronger than the initial signal. Amplified signal is relevant for compensating the loss in strength of signal caused by resistance in the cable. Repeater works as a physical device, and it is important for long distance connections. [1, 202.]

Hub is another example of physical device which has no ability for decision making. Hub has similar functionality with repeater, but the signal is duplicated for different ports. Switch is often confused with hub, but the main difference between them is the intelligence, switch has it and hub does not. Hub is not relevant equipment for designing modern networks, it is covered in this work only to highlight that it should not be confused with switch. [1, 202-203.]

Switch is a device that usually performs forwarding based on MAC address, but some switches can do routing too by IP address information. This means that switch can be placed either on the data link layer or the network layer on the OSI model. Switch uses MAC address table to memorize the location of a specific device, and it forwards frames based on the table. [1, 205-209.]

Router is using routing table for storing IP addresses and routes to different networks. Routers are placed on the network layer in the OSI model because IP addresses play a big role in functioning of router. Without routing the packets would not find their destination. Routers use default route as an alternative if the route is not found in the table. Dynamic routing is usually used in larger networks, where routers share their routing table automatically. This allows routers to automatically learn routes to unknown paths, and to use the most efficient path available to destination. Static routing requires more

manual configuration and it is beneficial only in tiny networks for avoiding redundant traffic, which is caused by updating routes in the network. [1, 209-213.]

2.5 Physical Medium

Cabling is one part of the hardware, which has a significant impact on the network. Usually in industrial applications there are two types of cable used, copper and fiber optic cable. In practice, both copper and fiber are needed to keep the costs moderate.

In fiber optical cabling, light is used for the transmission of data, which enables high speeds, even up to 40 gigabytes per second. Fiber optic is immune to electromagnetic interference, as it uses light for delivering the signal. For the light traveling in the cable, glass is used as a reflector, which makes fiber optic cable prone to fractures. [2, 28.]

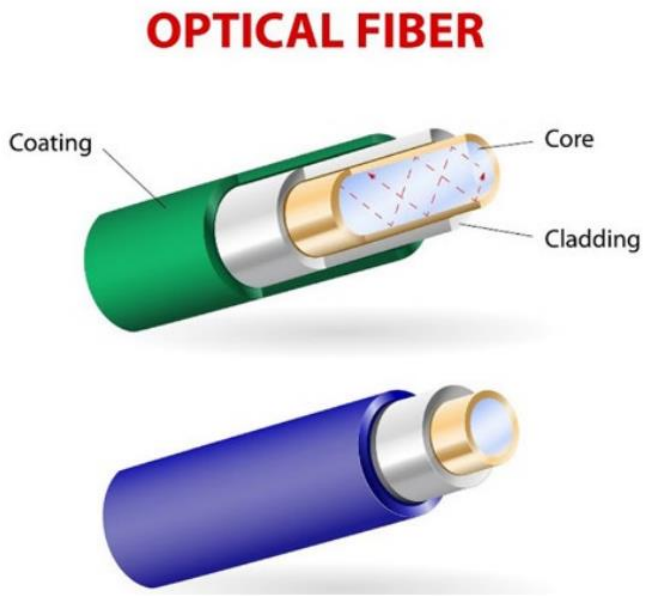

Figure 3 Structure of Optical Fiber [2, 28].

Structure of fiber optic cable can be seen in figure 3, which consists of several layers because it would otherwise break too easily. There are two types of optical fiber cables, Single-mode fiber (SM) and multi-mode fiber (MM). Distinction between SM and MM is in the structure, which has an impact on capabilities of the medium. As the name implies, SM uses only one beam of light, whereas MM uses several of them. SM is not only

capable of higher speeds but also more stable transmission with less restrictions on the distance. The advantage of MM is that it will not require as accurate light as SM needs. [2, 28.]

Twisted pair cable might be more familiar for most, because it has registered jack (RJ) connectors, which is used in computers and other devices with wired network. Copper cabling is usually used for short distance communication because high speeds can be achieved, however with restricted distance. Benefits of copper cabling is the low price and sturdier structure than optical fiber and it is common in LAN environment. [2, 25.]

Figure 4 Shielded twisted pair cable [2,26].

Twisted pair cables are available with shielded and unshielded versions, as figure 4 illustrates, shielded cable has an extra shield for electrical interference. Twisted pair cables also have different category ratings, which has an impact on transmission capabilities. [2, 26.]

2.6 Network Topologies

The layout of nodes in network is called topology, which describes the links between nodes and type of these links. Physical topology only shows the physical connections between devices, in other words it gives a rough idea of the network connections. Physical topology is beneficial for the mechanical installations and for physically locating the devices in large areas. Logical topology is more focused on the abstract perspective, it gives more specific logical information about the devices and their connections. Logical connections mean that the devices are not physically connected the same way as they

function. Properly designed topologies make network run more efficiently and reduces time used for maintenance operations. Every application should be considered as its own, and there is no universal topology that would cover all problems in networking. There are variety of topologies and combination of topologies called hybrid topologies, hybrid topologies are not further covered in this thesis. [1, 91.]

2.6.1 Bus Topology

A device in bus topology sends the message to both directions and goes through every device in the way to find the destination. If the message is not meant for device, it is passed to the next one and ignored. Device examines the message and decides by IP address or MAC address, if the message is meant for it.

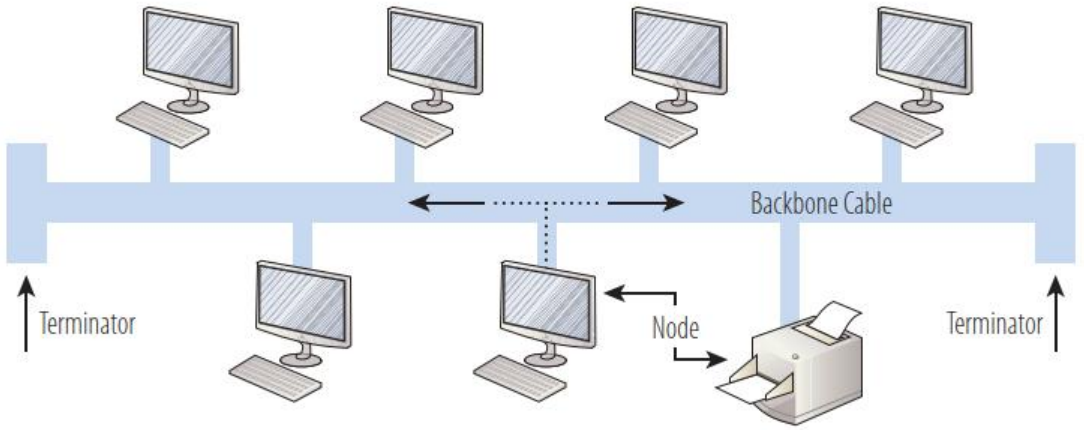

Figure 5 Bus Topology [1, 92].

Bus topology is one of the simplest topologies, it uses backbone cable to send data between devices, as shown in figure 5. The backbone cable should include a terminator for keeping the signal from bouncing back at the end of the cable. The advantages of a bus topology are all related to the simplicity of the topology. It requires no additional devices or other expensive parts, and it is easy to execute. [1, 92-93.]

2.6.2 Ring Topology

In a ring topology message sent by the device is going through all the other devices before the destination computer, if another device gets the message it is passed forward before it finds the targeted device. [1,94.] If used in a switched network, ring topology requires a protocol to prevent packet loop from happening, for example Spanning Tree Protocol (STP), which is covered later in this work. STP also makes redundancy possible when using switches, redundancy makes it more reliable topology [4].

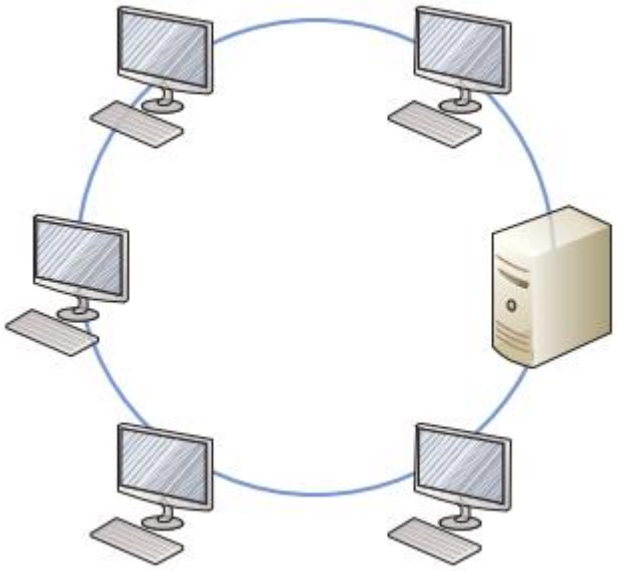

Figure 6 Ring Topology [1,94].

As seen in figure 6, the name of ring topology describes the layout of nodes in ring topology. Devices are connected to each other consecutively, creating a closed loop. Benefits of ring topology is free from collision problems and adding large quantity of devices is not expensive. Regardless of advantages, in case of failure of any device or cable the whole network is down if redundancy is not used. Finding the cause of failure might be challenging, which is another issue in a ring topology. [1, 94.]

2.6.3 Star Topology

Star topology is a common topology because it is used in office area. Star topology has one central device working as a master device and other nodes connected to the hub as

slaves. Any data send in star topology goes via the central device, which processes the data and send it forward to the destination. [1, 94-95.]

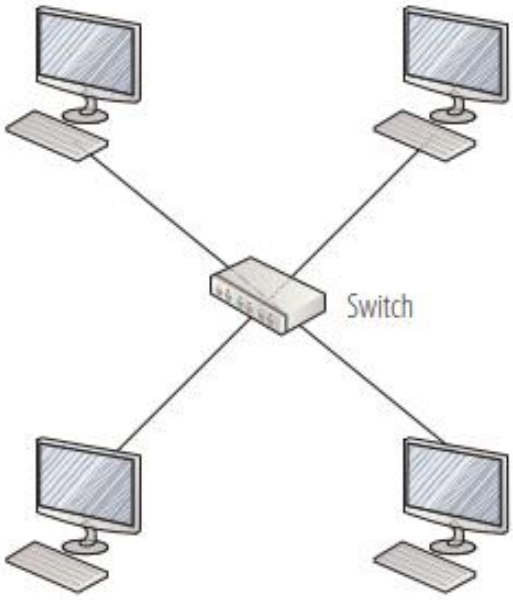

Figure 7 Star Topology [1, 95].

The layout of star topology is shown in figure 7, hub could also be replaced with a switch in star topology. The forwarding depends on the hardware used as the central device. As covered earlier in this work, a switch has an ability to target the data only for the desired node, but a hub just duplicates it for every node. Either solution will work, because only the wanted node will pay attention to the message. Because a hub works by sending the message to every node, it will cause unwanted traffic that leads to loss of the performance. Using central device allows to other nodes in network to work properly even if one cable is broken, and central device also helps with maintenance operations. Star topology has no performance issues with a switch as the central device, but with a hub performance is diminished. There are still drawbacks too, the amount for devices in star topology are dependent on the central device. [1, 94-95.]

2.6.4 Mesh Topology

Mesh topology is a proper solution, if financial aspect is not considered. It requires a lot of cabling and time for designing and installing the network. Every device also requires

additional network cards, the quantity of network cards per computer depends on the size of network.

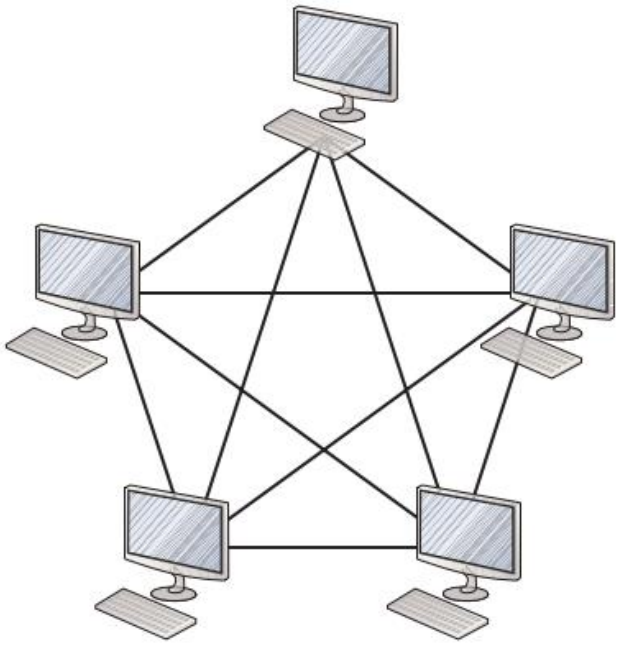

Figure 8 Mesh Topology [1, 96].

Figure 8 illustrates the connections between computers in a mesh topology. Every device has its own link to every other device in the network. This allows nodes to communicate via alternative routes by utilizing the connections between other nodes, which is useful in case of broken cable or device. Drawbacks of mesh topology are high costs and it is not realistic to build a large mesh network. [1, 96-97.]

2.7 Networking Security

Networks use variety of solutions for preventing unwanted events by restrictions. Restrictions can be executed physically, logically and by software. Usually restrictions relate to incoming traffic, but it is also important to consider what information can be sent out. Only the most relevant solutions are explained in this work.

Firewalls determine the trustworthiness of traffic and controls the flow to different directions. Firewall can block users from accessing the network, or it can inspect the data sent and decide if its legal. [5, 216-217.] Subnetting is also used to classify the authority of users, which was covered earlier in this work. From security aspect subnetting is used for dividing networks by user roles, which prevents unwanted users to access a specific network. Virtual Private Network (VPN) is also something to bear in mind, VPN uses its own private path for reaching the destination network [5, 12]. One practical example of VPN is remotely accessing files between different networks. There are also various algorithms and software for reducing the security issues.

3 Industrial Ethernet and Automation

3.1 Ethernet Versus Industrial Ethernet

Definition of Ethernet was explained earlier in this thesis, Industrial Ethernet has more requirements than commercial Ethernet. Physical conditions in industry differs from normal office or home environment. Errors or delays in data transmission is not as crucial in office or home networks as in industry. These factors must be taken into consideration when implementing Industrial Ethernet, hardware and software both differ in industry and office environment. [6.]

Usually manual usage is minimized in automated processes, this differs from using a computer in office network. When using a computer in basic conditions, someone is giving commands for the computer continuously. In an automated process, command is usually given once and then the equipment runs automatically. When an error in delivery of a message occurs, in a home or office environment the user can try to run the command again without any rush, in industry on the other hand it is not that simple. Commonly there is not much time to react when something goes wrong in industrial environment, in other words it is crucial to deliver the message in a short time for the receiving end. Handshaking is a method used for ensuring the delivery of the message for the receiver. The controlling unit sends a query for devices and waits for them to answer, the message is re-sent if it is not answered. [6.]

Next thing to consider is the physical stress factors in an industrial environment. Not only cables are prone to get damaged by harsh conditions, but also other hardware tend to suffer. Improper temperature or humidity will reduce the lifespan of equipment, which cause unwanted costs and unpredicted errors. Not all industrial sites are indoors, weather has a big influence in the conditions outside. Outside might be cold, which leads to fractures in cable over time if cable does not fill the requirements. Not only cold but also heat can weaken the quality of cables over time. There are variety of other devices in industrial environment, and majority of them use electric signal of some kind, and additionally make vibration. Other devices should be taken into consideration because they can interfere the signals and by vibration make physical damage to cable or other hardware, if not properly installed. Using adequate equipment and covering them properly is crucial in industrial ethernet. [6.]

Industrial applications have different requirements, which leads to differences in topologies and overall equipment used. In office environment star topology is mainly used because it is suitable for most office areas, due to their lower requirements compared to industrial applications. Star topology is not applicable option every time in Industrial Ethernet, that is why industry uses many different topologies. Industrial ethernet has different classes for endurance of equipment, differing from light to heavy. Class of hardware and cabling is determined by environmental factors. It is not recommended to use light duty hardware in harsh environment, but on the other, hand using too heavy hardware is not cost-effective. [6.]

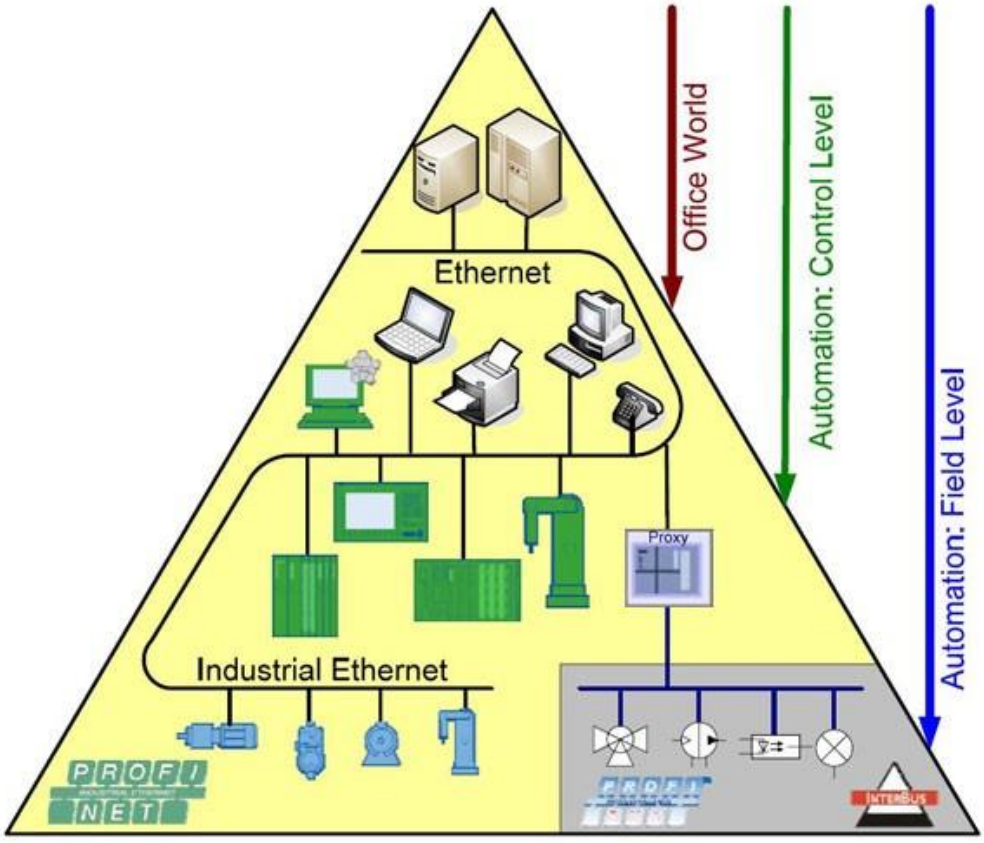

Figure 9 Industrial Ethernet in Automation [7].

As shown in figure 9, Industrial Ethernet is used for communication closer to field level than standard Ethernet, they locate on different layers in hierarchy. Control level devices utilize Industrial Ethernet for communication between field devices. Another option for communication is using fieldbus, which is more traditional solution. By using proxy, it is possible to convert Ethernet data to fieldbus data and vice versa, which allows simultaneous usage of both protocols. Industrial Ethernet is significantly faster than fieldbus but limitations of Ethernet relate to compatibility and maximum length of cable [8].

3.2 Industrial Ethernet Protocols

PROFINET IO is a protocol used for real-time communication between field devices over standard Ethernet protocol, it is derived from PROFIBUS, which is a fieldbus by the same manufacturer, and they share many functionalities. PROFIBUS and PROFINET IO both use cyclic data transmission, but PROFINET IO uses it via Ethernet, whereas

PROFIBUS is using serial communication. Benefits of PROFINET IO are based on the high speed, and it can be used in many applications effortlessly. [9.]

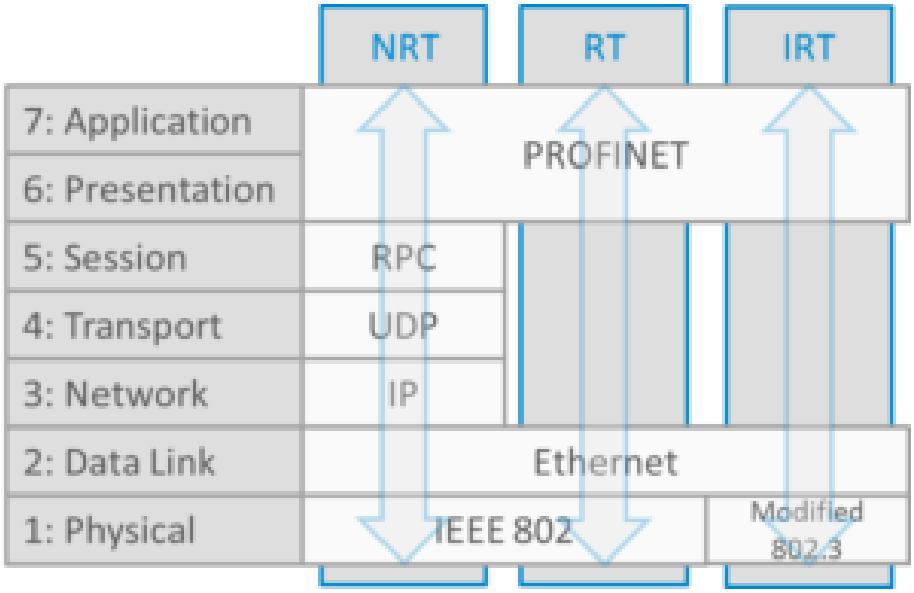

Figure 10 PROFINET OSI-model [10].

As shown in figure 10, PROFINET is cut in three channel types, where the real time communication channels use only the mandatory layers of OSI model for data transmission. Non-Real Time (NRT) channel is not using real time communication, because it must use IP addressing for hopping over different LANs. Real Time (RT) channel is using basic IEEE802 standard on the physical layer, whereas Isochronous Real Time (IRT) channel, has modified version for the IEEE802.3 standard. Practical difference between the real time channels is that IRT has optimized for applications where jitter and latency must be close to zero. IRT got the ability to tell switches to prioritize PROFINET traffic, which is the reason it has the lowest jitter and latency of these technologies. Conformance class C is required for IRT. [10.]

	A	B	C
Real-Time Data Exchange – cycle times down to 1ms	☑	☑	☑
Alarms and Diagnostics	☑	☑	☑
Network Topology Support	☑	☑	☑
SNMP Support		☑	☑
Rea-Time Data Exchange – cycle times down to 31.25µs			☑

Figure 11 Conformance classes [11].

Figure 11 indicates the specification of different conformance classes in PROFINET network. Conformance class sets rules for device requirements that help to choose the right equipment for a network. Time-critical applications, such as robotics might have more strict requirements in latency. Controllers and field devices must have PROFINET certification in every class. Network devices in class A does not require the certification, but in other classes it is mandatory. [11.]

Ethernet/IP is an Industrial Ethernet protocol, which also uses standard Ethernet principles. Using the standard Ethernet allows Ethernet/IP to connect with any other standard Ethernet-based devices, and it will follow the development of other technologies. Ethernet/IP is used to allow Common Industrial Protocol (CIP) information to communicate with traditional Ethernet protocol. CIP is an industrial protocol for exchanging object-oriented data between devices, which includes information related to manufacturer and identification. Ethernet/IP is difficult to implement because it requires knowledge of IT and automation technology. [12.]

MODBUS TCP/IP is an open protocol, which uses TCP/IP for communication, TCP/IP covers several protocols that make sure the message is delivered to the wanted destination properly. [13]. MODBUS TCP/IP uses master and slave for communication, which

means that slave devices do not make anything without the command from master device. Master device is usually some kind of device used for operating the slave devices, for example an operator sending a command from an operating panel for a field device. Master device waits for a response from slave after the message is sent. [14.]

EtherCAT uses pass-through reading, meaning that the data is read and modified by each node in the sequence before it is passed to next node. Like MODBUS TCP/IP, EtherCAT is using masters and slaves for communication, master sends a message and it is passed on by slaves, and the outcome is that the master will receive the message. Pass-through reading allows the data to travel without clear interruptions, which makes EtherCAT high speed protocol. EtherCAT is aware of the current time, which allows it to make the communication stable. Time awareness allows the master device to make assumptions about the time consumed for the next message sent based on earlier delays. Master device in EtherCAT connection does not need big investments, but the slave devices on the other hand does. Overall costs are not excessive, because most of the hardware has no strict requirements, and it is compatible with many topologies. [15.]

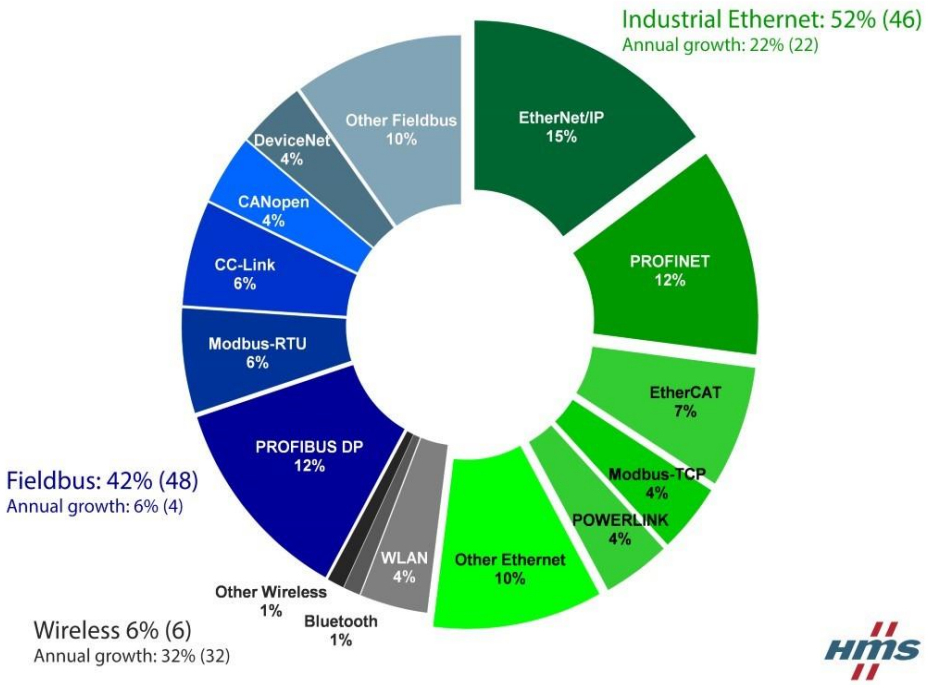

Figure 12 Industrial network market shares 2018 HMS [16].

Figure 12 shows installed Industrial Ethernet devices compared to traditional fieldbus devices, Industrial Ethernet has taken the lead over serial-based fieldbus systems by 10% in 2018. According to HMS, it is predicted that the number of traditional serial-based fieldbuses installation is going to diminish, and wireless technology and Industrial Ethernet will take over the market.

3.3 Industrial Automation in General

Industrial automation is invented for reducing mechanical work done by people in industrial applications. Automation reduces incidents in workplace and makes the process run more efficiently. Automation systems consists of different levels, and every level has its own functions. There is no one specific solution for every industrial application, there are many solutions for controlling or interfacing with machinery. An example of hierarchy in industrial system, and the requirements on different levels can be seen in figure 13. The structure of automation systems is not the same in all companies, but figure 13 is used for illustrating the basic structure.

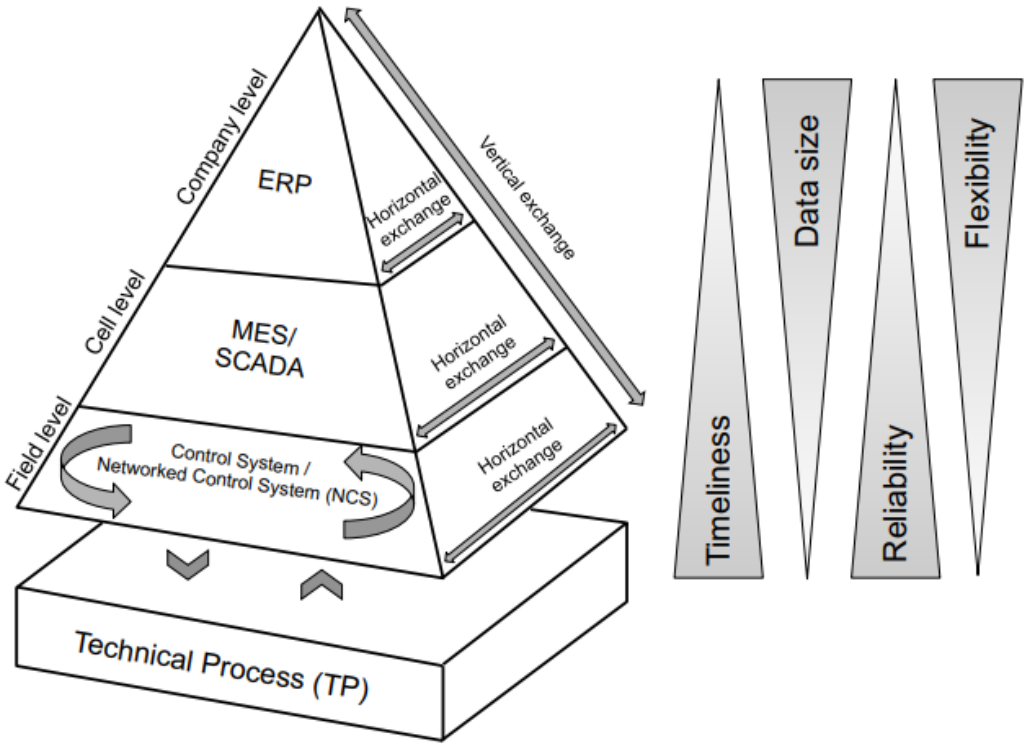

Figure 13 Automation Pyramid [17, 9].

As shown in figure 13, field level on automation pyramid is closest to the actual process, which includes field devices. Field devices can be for example sensors or actuators that convert physical measures to electrical signal and vice versa. Sensors are used for measuring data for the controllers, and actuators are used for physical movement when needed. For example, a pressure sensor can sense that pressure is too high, and then an actuator can move to open a valve for releasing the excessive pressure. Reliable and predictable communication are most crucial factors on this level because they have an impact on safety and timing of the applications. [17, 9-10.]

Sheer field devices cannot do actions without commands, which is why there are control systems in automation. Controllers acquire information about the process directly from the sensors, and they can send commands for actuators based on the sensor data. Controllers usually receives the data in cycles, the cycle time depends on the requirements of the specific application, for example robotics and other real-time applications require lower cycle time. [17, 9-10.]

On cell level, people start to interact with the machinery. Cell level is where supervisory happens, operators give manual commands for devices via controllers. Manufacturing Execution System (MES) is also at this level. [17, 8.] MES is a system for monitoring different factors related to manufacturing, and to automatically reacting for changes. This prevents confusion caused by people because it has all information about maintenance, resource optimization, and every other important data about the manufacturing. Decision making is made in real-time, which differs from the traditional human interaction. [18, 37-41.]

Company level is the closest level to outside world from the company. Most of the financial decisions are done at this level. Enterprise Resource planning (ERP) system is used for these functions. This kind of system not only helps customers with better services, but also assist employees with real-time information about incoming changes outside the company. [18, 43-46.]

3.4 Control Systems

There are differences between control systems of automation equipment. Most widely used control systems are Programmable Logic Controllers (PLC) and Distributed Control Systems (DCS). While modern PLC and DCS share basically the same functionalities, they still do differ from each other. [19.]

PLC is optimal for fast response time requiring applications, such as robotics, because a small delay will mess up the process. Due to slow response time of DCS, it does not use its own controller for safety functions, but PLC does. [19.] Other benefits of PLC are related to the software, which helps with diagnostics and allows to customize the features of PLC [20]. PLC is beneficial, when control must be fast, but there it is not as reliable as DCS.

DCS is more optimal for larger applications with higher requirements in reliability. DCS is a robust system, and it can connect a large quantity of I/O devices, which is something that a PLC cannot do. [11.] DCS can be modified on the run, which allows all processes to run while upgrading the system. Basically, DCS is beneficial for large processes that cannot be down for a long period of time. [20.]

3.5 Risk Assessment

Automation machinery use a lot of mechanical power and can carry heavy objects, leading to a risk of accidents in the workplace. Safety functions in automation is thereby crucial part of design and implementation for preventing accidents. Risks must be minimized as much as possible to the stage where accident is not likely to happen. Risk is evaluated by the combination of probability and the results of an incident. Risk does not only apply to human related accidents, but also for machinery or even harm to financial matter. Risk is minimized by systematic approach that is starting from identification and ending to monitoring. The risk assessment should not only include the designers, but also people who are relevant to the process. [21, 128-129.]

First phase is to identify the incidents that could be caused by natural phenomenon, human error or by defective equipment. The idea is to think about the whole scenario,

what could happen if something went wrong in the process. One minor error might cause a chain reaction and end up to a fatal incident. In other words, every small detail matter in the evaluation. [21, 128-129.]

After potential incidents are found, they must be evaluated further. Two factors must be considered, how severe accident could they lead to, and how likely it is to happen. The outcome can be determined for example by doing a matrix, where the results are a product of these variables. The matrix has different stages for actions required that depends on the result from multiplication of two factors, probability and consequences of an incident. The result is based on the coefficients of the two factors, and they have their own criteria. [21, 129-130.]

When the risks are defined, next consideration is to plan actions for decreasing the risk level, which could be done by reducing the odds or the consequences. Not all observations are fixed, and some of them are postponed if the risk is not high enough. Risks can be diminished for example by restrictions, automation, or modifying the existing process. After the required actions are done, they must be re-evaluated, and possibly altered again if needed. When all changes are done, it is essential to monitor the solution for ensuring the wanted result. [21, 130.]

3.6 Atmospheres Explosible

Atmospheres Explosible (ATEX) is a directive used in European Union for concerning areas vulnerable for explosion. Basic idea of the directive is to prevent the initial ignition in ATEX categorized areas because the ignition would spread by flammable substance mixed with air. In other words, the purpose of ATEX directive is to remove every factor from the explosive areas, which could lead to ignition. Factors to ignition usually relate to the equipment used in the zone. [21, 59.]

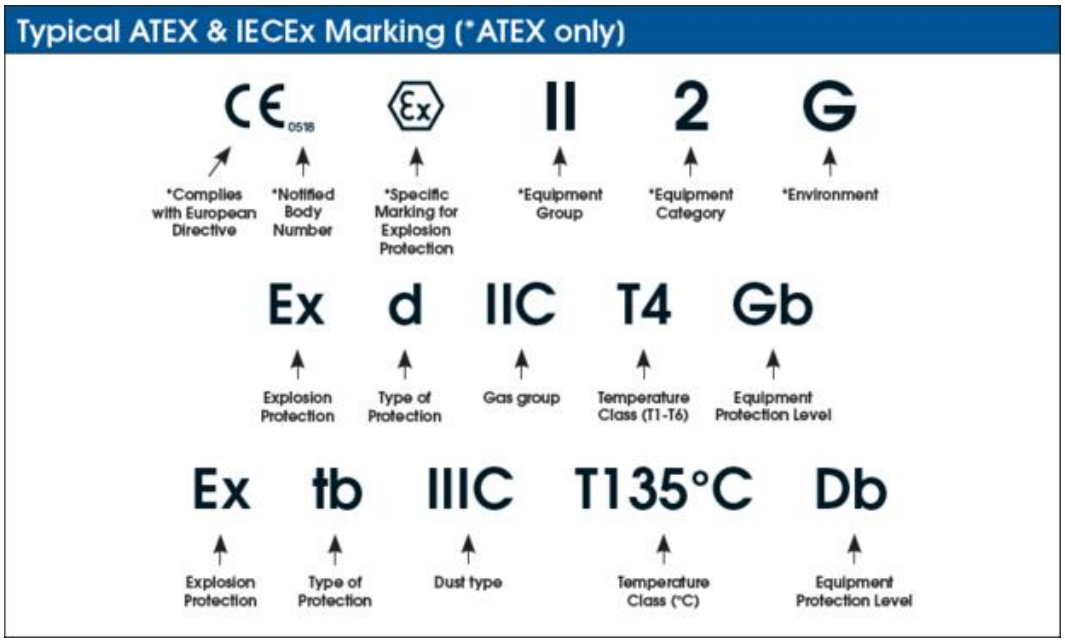

Figure 14 Typical ATEX and IECEx markings [22].

Figure 14 shows the most common markings related to ATEX zone equipment. Equipment are categorized by different factors, reason for categorizing is that some areas do not require as strict specification as others. Group is for defining whether the equipment is applicable for underground mines or other areas. Category defines what level of protection is required, which is determined by likelihood of explosion. Environment refers to the substance which is present in the zone, and substance is divided into gas and dust. Temperature is also essential because it could lead to ignition of substance mixed with air. In ATEX markings, temperature indicates the maximum temperature on the surface of malfunctioning device. CE marking is more generic acceptance marking than Ex marking, both are required for ATEX zone. Ex marking is the one, that defines more specific test acceptances. [21, 59-60.]

3.7 Industrial Automation Network Security

Crucial part in safety of a process is security of information transmitted in industrial applications. As covered in the networking chapter, subnetting is one way to improve security of a network, in industrial applications demilitarized zone (DMZ) is common way to separate the industrial zone from other networks. DMZ is used for preventing direct connection from unwanted networks to industrial network, which usually are enterprise and

the internet. The reason for using DMZ is mostly the sensitivity of information in industrial zone. Another factor is that the systems might be outdated in the factory floor, causing threat to information security that way. DMZ can be implemented by placing it between two firewalls. One firewall controls the traffic from enterprise zone, and other controls the industrial zone traffic. [23, 13-14.]

Performance is one security concern, networks in industrial applications require more stability than traditional networks. If the network overloads, it might crash the system, which is not only expensive, but can also be hazardous. Redundancy for critical systems is a simple way to avoid conflicts in shut down situations. Redundancy means using a secondary system, which starts if something goes wrong in the primary system. Redundant system can be implemented physically and logically. Physical redundancy includes cabling, redundancy protocols is discussed later in this work. If the aspiration is only to prevent hazardous events, one way is to prioritize the traffic. Prioritizing traffic means guaranteed transmission for critical information in a specific time. As covered earlier in this work, designing topologies correctly make significant difference in performance too. In this case, performance means latency and jitter mostly. Latency means delay of the message delivered, and jitter is the variation of the latency. [23, 14-16.]

3.8 Safety Functions in Automation

There are several devices used for ensuring safety in automation. It is important to take hardware and software into consideration. Devices concerning safety of the process include all industrial zone equipment, not only field devices. [24, 164-170.] It is crucial that the transmission of information is reliable and fast enough for ensuring rapid reaction by people on supervisory level [24, 171-172]. The equipment should be compatible with each other, and they should be tested before production in Factory Acceptance Test (FAT). FAT is used for ensuring the proper operability of the setup at the factory, including software and hardware. Further testing is done at the site with Site Acceptance Test (SAT). [24, 180-181.]

In process automation, it is common to use safety actions besides the actual safety devices. Actions involve manipulating valves depending on the situation, for example closing a valve in emergency situations. Actions could also be restrictions for preventing user

from operating the process in different conditions. This kind of actions are usually operated on a separate system because DCS is commonly used in process automation. Reason for separate system is that DCS lacks speed, as mentioned earlier in this thesis. Switches and other devices are used in processes to detect hazards, and usually actuators, such as valves are utilized for reacting to the hazard. [24, 102.] In factory environment, safety relies more on the safety devices and restrictions on motion. In factories the basic functionality is that if a sensor detects movement in danger zone, the process is shut down.

Safety Integrity Level	Probability of Failure on Demand	Risk Reduction Factor
SIL 4	$>= 10^{-5}$ to $< 10^{-4}$	100,000 to 10,000
SIL 3	$>= 10^{-4}$ to $< 10^{-3}$	10,000 to 1,000
SIL 2	$>= 10^{-3}$ to $< 10^{-2}$	1,000 to 100
SIL 1	$>= 10^{-2}$ to $< 10^{-1}$	100 to 10

Figure 15 Safety Integrity Level [25].

There is a reference for defining the safety level for a process, which is called Safety Integration Level (SIL), and it is shown above in figure 15. SIL level is defined by the probability of an incident, and the factor can be used for determining the effect of an improvement. A piece of hardware does not give specific SIL, it is affected by the whole process. Regardless, one incorrect device can decrease the SIL significantly, which is why the SIL compatibility should be checked carefully. SIL can be increased by actions, which lowers the probability of an accident, for example with smarter devices that have diagnostics. [25.]

3.9 Industrial Safety Protocols

Most of the vendors have their own protocol for safety functions that have more strict requirements than the basic Ethernet-based protocols. Safety functions must have extra

low latency and it has no room for malfunctioning, which on the other hand applies to most functions in automation but to a lesser extent. Every protocol covered in this chapter meets the requirements for SIL 3 applications.

First protocol covered is openSAFETY, which in accordance to its name is an open protocol for safety automation. Open protocol makes it independent of Industrial Ethernet protocol used. The main benefit of this is the integration of different protocols in an industrial site. All safety related data is packed into a single frame, and all devices understand it without additional effort. The protocol cuts the data format in two pieces, which share the same data, and checks their integrity with different algorithms. An openSAFETY network is divided into domains, which can hold a large quantity of devices, and they can work as different safety zones. As the openSAFETY protocol enables to communicate with different Industrial Ethernet protocols, it has some disadvantages too related to the difference in functionality of different protocols. This means that the engineers have extra work to do. [26.]

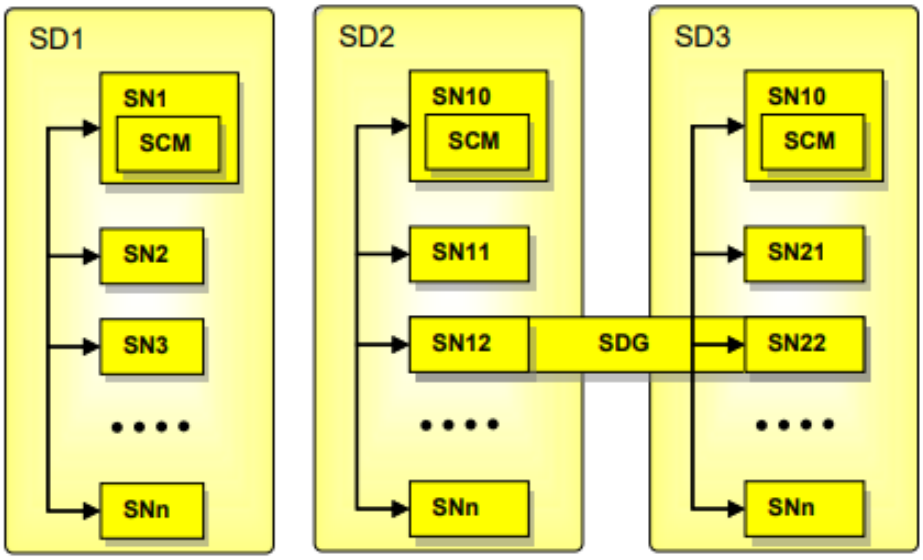

Figure 16 openSAFETY layout model [27, 26].

Figure 16 shows the basic logic behind the topologies of safety networks in openSAFETY. As shown in figure 16, for communication with different domains there must be a specific gateway device between Safety Domains (SD). In this case, SD1 domain cannot communicate with SD2 or SD3 because SD1 has no gateway device to reach other

domains. This should be considered when designing openSAFETY network, a special gateway device might bring the costs up if there are many domains.

PROFIsafe is a safety automation protocol compatible with PROFINET and PROFIBUS systems without additional effort. The main benefit of PROFIsafe is the simplicity of automation network. The automation networks in PROFIsafe are simpler because the protocol integrates safety functions with other functions. This improves the engineering and maintenance operations, since they are not as difficult to execute. Another advantage is that PROFIsafe does not care about whether the original system is using serial or Ethernet communication. PROFIsafe adds a logical layer for the safety functions, the layer is shown in figure 17 and it exchanges the data via PROFIBUS or PROFINET with one cable. While the data is passed, also the integrity of the data is checked by the safety layer. [28, 8-9.]

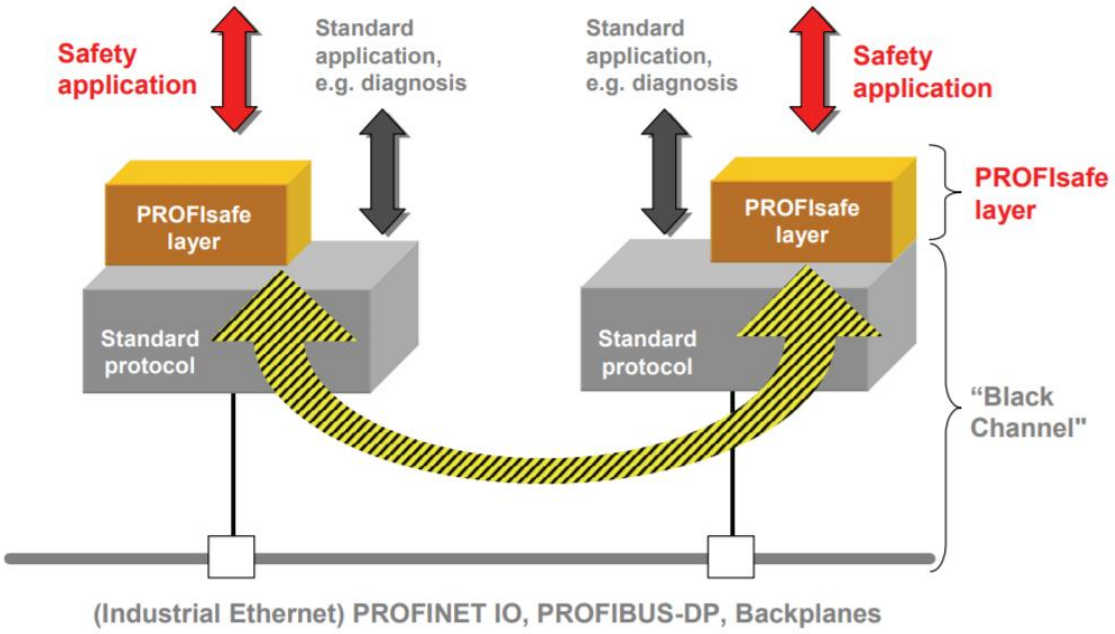

Figure 17 The Black Channel [28, 4].

In figure 17 is shown the logic behind communication in PROFIsafe, it uses “black channel” for the standard communication. Black channel communication is a technology which is capable of transmitting safety related data with the same medium as other data. Safety related data is still logically isolated from other data, which prevents them from

mixing up. Basic PLC and fieldbus can be used with the black channel communication with the existing cables. Black channel technology has similar purpose as VPN, but it is used for safety related industrial communication. [28, 4-5.]

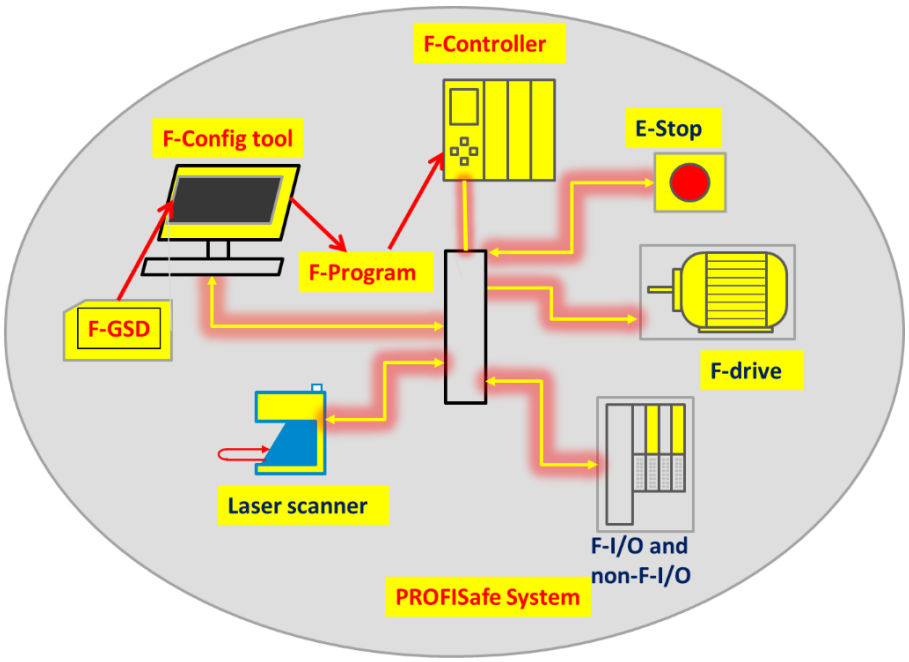

Figure 18 PROFIsafe layout example [29].

In PROFIsafe failsafe devices are called F-devices, in figure 18 is a simple layout of an PROFIsafe equipment. As shown in figure 18, safety I/O and non-safety I/O can be on the same system, but their functions are still separated. PROFIsafe needs an additional F-config tool, which must contain the configuration file for the controllers to operate with devices.

CIP safety is addition for CIP, which is a protocol for enabling different industrial ethernet protocols to communicate with each other. CIP also allows the protocols to communicate with higher levels of industrial hierarchy. CIP safety is used for safety applications for example in Ethernet/IP, DeviceNet and SERCOS III. As in earlier protocols mentioned, CIP safety also enables to combine different protocols by using an additional layer for safety functions. In CIP safety the investments are rather done to the end devices than the routing devices. The routing devices are responsible for checking quality of the

message, and for reacting to the deviation in data transmission. Benefits of CIP safety is the possibility to make large safety applications without high bandwidth requirements, and the flexibility of data acquisition on different levels in the hierarchy. [30.]

Safety over EtherCAT is used for the safety functions over EtherCAT protocol, and it adds an additional channel for the safety functions like the other protocols mentioned above [31, 8-11]. EtherCAT has separate safety I/O modules and devices, which include masters and slave, such in EtherCAT [31, 14-16]. Like in other protocols, FSoE also guards the frame sent, where the master sends it and waits for a response from the slave [31, 17-19]. FSoE is also compatible with many other fieldbus systems, including serial communication and ethernet-based communication [31, 26].

4 Emerging Technologies

There are several discussed topics related to industrial automation which are on development, and not yet ready for every application. Relevant for this thesis are technologies which have an impact on safety or security. The fourth revolution of industry is digitalization of all devices and functions with intelligence for seamless communication. There have been three earlier revolutions in industry, which has developed from steam machines to electrical, and from electrical to digital electronics. Internet of things is one part of the fourth revolution. [32, 4-6.]

Internet of things (IoT) is an idea of automatically collect every relevant piece of data from all devices connected to networks, including physical devices. After collecting the data, it is utilized by algorithms, usually in a cloud-based system. One benefit of IoT technology is the integration of devices in different networks, which make them to communicate with each other without people. System makes real time decisions and conclusions independently, and it converts the data into understandable form for people. Today IoT can be seen in everyday life of people, for example in mobile device applications. [32, 6-7.]

Big data analytics are used for defining the large amount of data collected from devices. As a bunch of data is collected from all devices, it is essential to know what the data contains, and what to do with it. There are four main factors to consider when handling

big data. First question is how to handle the amount of data, because the quantity of incoming data is huge. Second thing to bear in mind is the rapid reaction to the data, real time information cannot have too high latency. Third factor is variety, all data is not in the same form, and some of it is difficult to handle. Another thing related to variety is the algorithms, which should be able to understand the influence of specific piece of data. Lastly, quality of data is difficult to determine, because of errors occurred in transmission of data. [32, 13-14.]

Industrial Internet of Things (IIoT) is similar idea but it is used in industrial applications. Comparison of IoT to IIoT is similar with the comparison of commercial ethernet to industrial ethernet, which was covered in this work earlier. Since industrial applications has no room for huge errors, the requirements of IIoT are stricter than IoT. IIoT is not as visible as IoT yet, but it is predicted that it will grow in the future, and it will have an influence on the way that systems work in society. The basic idea in IIoT is to add a cloud level to automation hierarchy, and to integrate the functions of every level. They data is processed in the cloud level. Real time reaction in the field level based on metrics outside the plant automatically is one example of the outcome of IIoT. The current integration of hierarchy is usually executed in a way that only the most relevant levels of hierarchy communicate directly with each other. [32, 40-41.]

Security impacts of IoT has many aspects. Firstly, all devices connected to IoT based system must be secure, and compatible with IoT. This has been an issue because of the marketing models that has forced the products too early on the market without proper testing and development. The main reason for this is the excessive hype of IoT, and it has driven the manufacturers to just prove that they have devices compatible with IoT. This had a bad influence for the development because the equipment really had no use yet, and still manufacturers was focused on getting the products on the market but not on improving them. [33, 35-37.]

Another security threat relates to integration of Operational Technology (OT) and Information Technology (IT). OT is the technology for operating the process directly, and IT is at the higher level of hierarchy. Integration of IT and OT allows hackers to access the operational environment if it is not carefully designed. OT information is usually the most crucial part of organization. OT security has been designed in a way where security has not been a top priority. History behind security issues derives from the fact that OT was

not originally connected to the outside world, this is restrictive factor in the integration. In the OSI model, communication protocols differ basically in every level when comparing OT and IT. [34]

Next technology discussed is the Fifth Generation of cellular technology (5G), which is also widely speculated in the industry. 5G is also a technology which is designed for both industry and consumers. Cellular networks are basic technology today, but they are improving all the time. 5G is the fifth generation of cellular networks, and it is influenced by IoT. The former generation is 4G, and it is predicted that 4G cannot handle the volume of devices in the future. 5G is still an incoming technology, which is not widely used yet, it is still missing standardization and other important factors. The aspiration for 5G technology in the industry is to make devices in industrial applications to work reliable. The devices should also function almost in real time as an ecosystem wirelessly with low costs. [35, 31.]

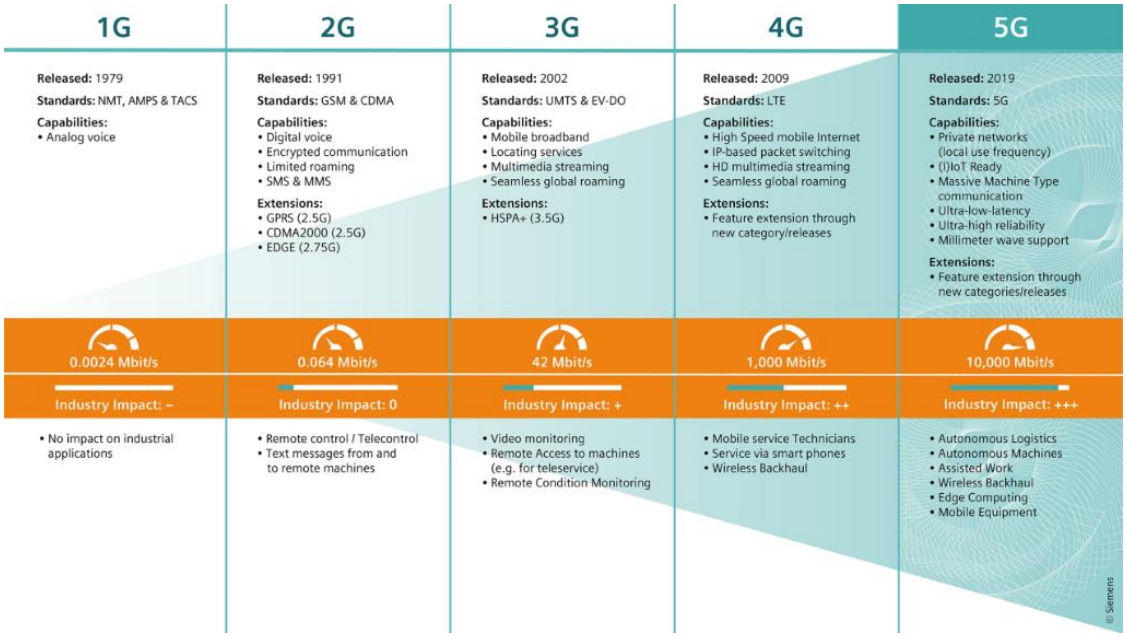

Figure 19 Comparison of different cellular network generations [36].

As shown in figure 19, 5G has many benefits over former generations, especially in industrial applications. As covered in this work, reliability and low latency are huge factors

in real time applications. As shown in figure 19, low latency and reliable connection are possible with 5G technology. 5G also enables to use own network with 5G technology, which makes it a private network wirelessly with less interruption than WLAN because of the higher bandwidth.

The basic idea of 5G is to focus more on the density of users in a specific area, rather than the distance of transmission. 5G consists of different existing technologies, which forms radio access network, core network, and end to end system. Radio Access Network is the technology used for LAN kind of technology with radio waves. [35, 37]. Core network is the spot that enables different parts of network to communicate with each other [35, 44]. End-to-end system is a technology for communicating between devices without routing or gateway equipment for more reliable transmission of data [35,47]. All the covered technologies still have some deficiencies, but the problems already have possible solutions with proper development.

As history has shown, wireless devices are not plain to implement from the security aspect. 5G is not an exception, the quantity of threats is just increasing all the time because more crucial data is delivered with wireless networks than before. It is difficult to determine whether the data is necessary or not. If the excessive data is delivered, the network starts to suffer from too much information. Solutions which are thought to solve these problems relate to intelligent decision making and encryption of data. [35, 79-81.]

Next technology covered in this chapter is Time Sensitive Networking. TSN is described as an Ethernet-based technology which is also fast and reliable like Industrial Ethernet protocols. Main benefit of TSN over Industrial Ethernet technologies is the precise prediction of how much time passes on a specific function, jitter and latency are big factors in TSN. This kind of technology is crucial when even a minor variation in transmission affects the process. [37, 2.] Addition to Ethernet, TSN is more flexible technology, and it is the able to match the strict functionality related to timing with its accurate scheduling [38, 10].

Time Sensitive Networking has different priorities for frames, where real-time traffic has high priority. TSN uses technology called Time-Aware Scheduler which uses cyclic communication that allows TSN to prioritize the transmission by pausing the cycle. Lower priority data is paused for delivering the higher priority information first. Addition to

traditional ethernet priority, TSN has more adaptive prioritizing of traffic and timing is more precise. Gate Control List is used to check and control the traffic. [38, 10.]

TSN frames are cut into smaller pieces, and they are delivered one by one, pieces of frame are called framelets. Reason for cutting frames to smaller pieces is that not all data is easy to predict. Another reason for cutting frames is the larger frames that require processing. If the processing of large data would start at the wrong time it, would lead to unwanted delay. If the frame is cut in pieces, they can be partially completed and then on better time. [38, 11.]

Regardless of the reliability of TSN, it still has quite crucial errors for implementation. TSN requires very precise configuration, even one device in the network can have a negative impact on the whole process, but there are incoming technologies for this matter. TSN is also one technology which is in the development phase, and it is not ready yet. But in the future, it might have a positive impact on the security if it is completed as it is described. [38, 11.]

5 Considerations of Ethernet Technology in Safety Automation

5.1 Requirements and Restrictions

There are some restrictions between different vendors, but they can be solved by using vendor independent protocols. Even with open protocols, it is not effortless to use different manufacturers in safety related networks. Extra costs come from engineering or purchasing the equipment. This means that it is possible to use different protocols together, but when it is viewed from financial perspective, the benefits depend on the application.

As discussed earlier, there is no guarantee for using brand new technologies without sacrificing the information security. In other words, it might not be ideal to use them for safety functions, as they have no room for errors. This does not mean that they will not be ideal for safety functions in the future, as the security issues are improving for these technologies all the time.

PROFIsafe network should meet the SIL 3 requirements. However, according to PROFIsafe system description there is no restriction for the type of switches used in network, but the limit of them connected consecutively is 100. Moreover, the F-address spaces should not be equal with each other. [28, 5.] Devices from different manufacturers on PROFIsafe island must be conformity tested to PROFIsafe requirements, testing includes availability testing but also safety testing for International Electrotechnical Commission (IEC) 61508 standard conformance. [28,10-11].

According to FsoE system description, FsoE has no restrictions for using other vendors equipment to transmit the data. FsoE also has its own conformance test system, and the devices should be applicable to FsoE conformance [31, 32]. Additionally, Devices used in Safety over EtherCat should be in accordance with basic safety function IEC standards. [31, 29-33.]

All openSAFETY nodes should have unique logical addresses inside Safety Domain. Physical address must be unique even outside the SD, overlapping addresses is recognized automatically by openSAFETY protocol. As already mentioned, openSAFETY communication between different domains requires a specific openSAFETY gateway device, which is one drawback of this protocol.

If the application is in ATEX area, the devices used in the ATEX zone should be compatible with used protocol. Additionally, devices must fulfill specification of the specific area, more specific information about the requirements can be seen in chapter 3.5. Not only the devices but also medium used must meet the requirements for ATEX directive.

For automation designers alone, it might be difficult to design automation systems by using ethernet-based protocols. Automation designers should have a basic understanding of networks, or they should seek for assistance, especially in safety related applications. Even the requirements mentioned above include network related restrictions.

5.2 Benefits of Using Ethernet-based Safety Protocols

The main benefit acquired from using Industrial Ethernet safety protocols is that integration to basically any system without adding any additional cabling or other hardware is

possible. This will have an impact on the overall costs of implementing a safety related network.

As covered earlier in this thesis, black channel technology is used in safety protocols, which utilize Ethernet protocol. This means lower costs for cabling and other hardware used in protection of safety related data, as it uses the same physical medium, which is isolated logically. Possibility to integrate with existing systems regardless of communication protocol used also brings another financial benefit for using Industrial Ethernet safety protocols, because the quantity of needed is additional hardware is low. Although the integration might be possible, the time used for migrating new system to an existing one should be regarded as an expense. The most effortless system integration occurs when the existing system is from the same vendor as the additional equipment.

Advanced diagnostics help operation and maintenance of devices, this brings lower downtime of equipment [33]. Easier maintenance is important because any system requiring safety functions will not operate before all the issues with safety equipment are fixed. Better Diagnostics means lower costs for maintaining processes operating.

Besides the financial benefits, development of the standards is also advantageous, as Ethernet is used also by consumers. This means that if something groundbreaking happens on basic ethernet protocol, it might bring something new to industrial applications as well.

5.3 Proper Recovering with Redundant Network

The collaboration between automation and ICT designing is crucial, especially when talking about safety functions. ICT designers must know what kind of hardware and topology options to choose depending on requirements of the application. Higher availability can be achieved by using network redundancy. When using redundancy, the recovery time is a critical variable that should be taken into consideration because redundancy is useless if it is not recovering fast enough. There are two kind of redundancy types, dynamic redundancy and static redundancy. If the safety or other time critical functions cannot afford latency at all, static redundancy is the only option. But if low latency is enough, it can be achieved also with dynamic redundancy.

There are many dynamic redundancy protocols, in this work Media Redundancy protocol (MRP), Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) will be further covered. Dynamic redundancy protocols are more resource friendly than static redundancy protocols, for this reason they suit better for some applications. [17, 105-106.]

Media Redundancy Protocol is a dynamic redundancy protocol that has an advantage in speed, but it can only be used in a ring topology. Achievable recovery time for MRP is under 200 milliseconds depending on the vendor. Even under 5 milliseconds is achievable, but It should be noted that the maximum quantity of nodes in network is limited to 50 for achieving the lowest response time in MRP. [17, 105-110.] MRP has a master node called Media Redundancy Master (MRM), and other nodes are Media Redundancy Clients (MRC). MRM regularly sends a test frame to check for connection integrity. [17, 107.]

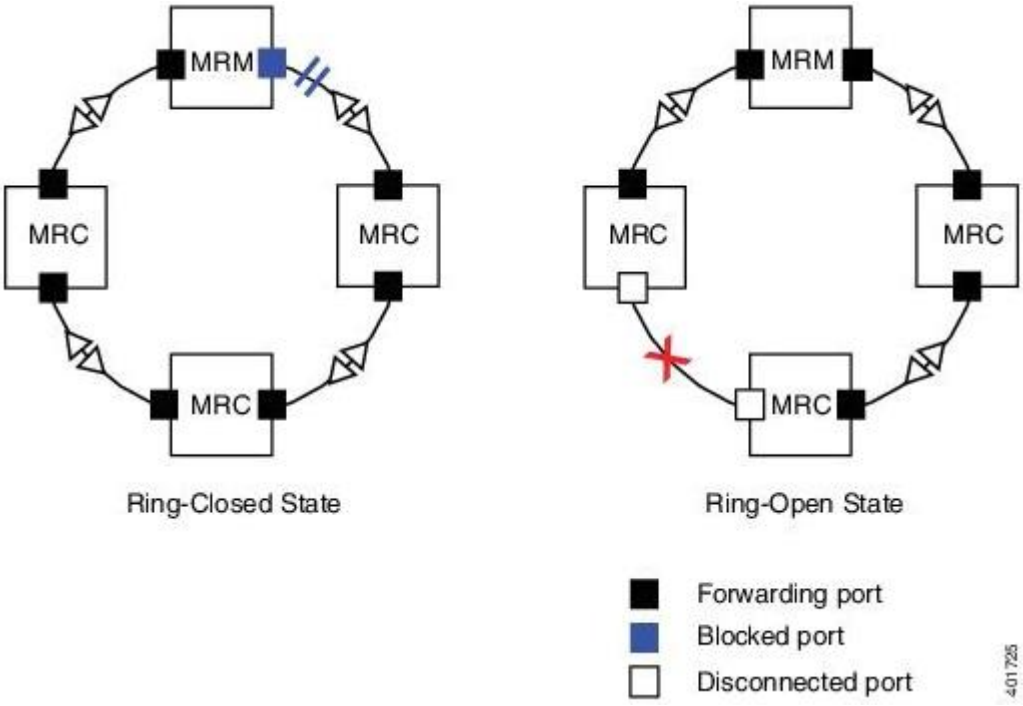

Figure 20 Media Redundancy Protocol [40].

As shown in figure 20, nodes have different states, depending on the operability of connection. In normal condition, MRM has only one port forwarding frames for preventing unwanted loop. Loop means that the message is sent over and over forward, which

cause excessive traffic and it floods the network. This is important when using Layer 2 equipment because they do not support time to live. In case of failure, the other port of MRM must be opened because it can reach all nodes, except the one with failure. This allows the network to run with redundant paths. [40.]

Spanning Tree Protocol is another dynamic redundancy protocol for preventing loops from happening, but with slower recovery time than MRP [17, 107]. In STP, one switch will be elected as a root bridge, which makes the decisions for the network, for example defining port states. Root bridge can be configured manually, or let the switches decide it automatically. After the root bridge is chosen, other switches calculate the best path to the root bridge, and the port is set as a root port. Other than root or designated ports are put in to blocking state. The root bridge sends hello messages regularly, which is ensuring that link is not broken. The main thing is that STP has too high response time for time critical applications, it can be tens of seconds. Rapid Spanning Tree Protocol is made to fix this issue with response time of milliseconds, and its functionality is similar with original STP. [2, 81-83.]

Examples of static redundancy protocols are Media Redundancy for Planned Duplication (MRPD), Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR). Lowest recovery time for static redundancy is zero. The reason why these recovery times are different is based on the different approaches in functionality. Static redundancy constantly checks, whether the system is up or down, whereas dynamic redundancy wakes up in a case of failure. [17, 105-110.] Type of a redundancy should be observed when designing a real-time safety critical system, as it has an influence on the whole response time of machinery.

Like MRP, Media redundancy for Planned Duplication is also used in ring topology but it has zero recovery time. MRPD sends two instances of a frame for both directions, both of frames include the same message. Sending the frame to both directions increases the probability of delivering the message to the receiver, because message has still another path if a device is down. [17, 56.]

Parallel Redundancy Protocol is another static redundancy protocol, one benefit being the variety of topology options. Such as MRPD, PRP sends the same message from two different routes at the same time, and if the receiver only gets one copy, it is reckoned

as a failure. On the other hand, if both copies of the message are received, only the first one is regarded. PRP can use standard switches because it is used by the end devices. [41.] High Availability Seamless Redundancy is similar with PRP, but it is physically implemented, and it is mostly used in redundant ring topologies. [42.]

Both redundancy types have their benefits but also deficiencies. There is no a best practice solution, every application should be considered separately. If the goal is to get zero recovery time, Static redundancy meets the requirements but if resources should be optimized or low recovery time is enough, dynamic redundancy could be considered as a preferable alternative. In most cases dynamic redundancy meets the requirements for recovery time. Applications, which could require zero recovery time are, such as safety functions that must work immediately after activation of a safety device, for example light curtains. Real-time applications that could have hazardous consequences in case of a failure, such as robotics might benefit from using static redundancy as well. Topology is another important factor when choosing the exact protocol for redundancy.

6 Conclusion

Ethernet technology has been developed from office area to harsh process environment for more demanding applications. This required some changes in the protocol, but it has successfully become popular option even for safety critical applications. The integration of automation and ICT is growing, and the distinction of them has become questionable. That is why cooperation between automation and ICT designers is becoming even more crucial, and both ICT and automation designers should have at least the basic understanding of both disciplines.

There are several technologies, which are not enough advanced yet for critical applications, but they might bring something new in the future. TSN is a technology to consider for safety automation, as it focuses on jitter and latency. IoT and other technologies related to integration might bring negative effects if it is associated with safety automation. IoT also might bring some unwanted latency from big data. Reason for security issues of these technologies are mostly because of the rush of bringing them into the market.

Ethernet technology brings significant improvement for modification of existing systems. Because the original system can be also serial bus system, it is not necessary to renew the whole system. Even safety related data can be transferred with the existing cabling. Another benefit comes from better diagnostics that help with maintenance operations. However, designing Ethernet-based safety system might require knowledge of information and communication technology. Network redundancy in network technology brings some advantages because of its flexible topology options, and advanced technologies. Concerning redundancy, dynamic redundancy is mostly proper option, but it is not enough in applications with zero response time.

The aim of this thesis work was achieved by using device descriptions, electronic sources, and other literature as references. The wanted results were gathered, and own conclusions were made, based on the references. Most of the references were from well-known companies, which makes the references more reliable. For further development of this thesis study, there could be a practical safety automation application that uses Industrial Ethernet.

References

1 McMillan T. Cisco Networking Essentials. Second edition. Indianapolis, IN: John Wiley Inc; 2015.

2 Carthern C, Wilson W, Bedwell R, Rivera N. Cisco Networks. Berkeley, CA: Apress; 2015.

3 study-ccna. Subnetting explained [online]. URL: https://study-ccna.com/subnetting-explained/. Accessed 10 October 2019.

4 Perle. Perle P-Ring Protocol [online]. URL:https://www.perle.com/supportfiles/p-ring.shtml. Accessed 12 October 2019.

5 Pérez, A. Network Security, Hoboken, NJ: John Wiley & Sons Inc; 2014.

6 Real Time Automation. Industrial Ethernet Overview [online]. URL: https://www.rtautomation.com/industrial-library/what-is-industrial-ethernet/. Accessed 13 October 2019.

7 Gonzalez C. MachineDesign. What Are the Differences in Industrial Ethernet Types [online]. URL: https://www.machinedesign.com/iot/what-are-differences-industrial-ethernet-types. Accessed 13 October 2019.

8 Bacidore M. Control design. Ethernet vs. fieldbus: the right network for the right application [online]. URL: https://www.controldesign.com/articles/2016/ethernet-vs-fieldbus-the-right-network-for-the-right-application/. Accessed 13 October 2019.

9 Real Time Automation Inc. PROFINET IO Protocol Overview [online]. URL: https://www.rtautomation.com/technologies/profinet-io/. Accessed 15 October 2019.

10 PROFINET University. Profinet Communication Channels [online]. URL: https://profinetuniversity.com/profinet-basics/profinet-communication-channels/. Accessed 15 October 2019.

11 PROFINET University. PROFINET Conformance Classes [online]. URL: https://profinetuniversity.com/profinet-features/profinet-conformance-classes/. Accessed 15 October 2019.

12 Real Time Automation Inc. EtherNet/IP Protocol Overview [online]. URL: https://www.rtautomation.com/technologies/ethernetip/. Accessed 20 October 2019.

13 Cloudfare. What is TCP/IP? [online]. URL: https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/. Accessed 20 October 2019.

14 National Instruments. The Modbus Protocol In-Depth [online]. URL: https://www.ni.com/fi-fi/innovations/white-papers/14/the-modbus-protocol-in-depth.html. Accessed 20 October 2019.

15 Real Time Automation Inc. EtherCAT Protocol Overview [online]. URL: https://www.rtautomation.com/technologies/ethercat/. Accessed 25 October 2019.

16 Anybus. Industrial Ethernet is now bigger than fieldbuses [online]. URL: https://www.anybus.com/about-us/news/2018/02/16/industrial-ethernet-is-now-bigger-than-fieldbuses. Accessed 25 October 2019.

17 Wisniewski L. Technologies for Intelligent Automation. Berlin, Heidelberg: Springer Vieweg; 2017.

18 Greeff, Gerhard, et al. Practical E-Manufacturing and Supply Chain Management, Elsevier Science & Technology, 2004.

19 Automationworld. PLC vs. DCS: Which is Right for Your Operation? [online]. URL: https://www.automationworld.com/article/technologies/dcs/plc-vs-dcs-which-right-your-operation. Accessed 1 November 2019.

20 Proctor M. Automation.com. DCS versus PLC in modern plant [online]. URL: https://www.automation.com/automation-news/article/dcs-versus-plc-in-the-modern-plant. Accessed 1 November 2019.

21 Pasman, H. Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals: A System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events, Elsevier Science & Technology; 2015.

22 Sinclair R. IEC e-tech. The hazardous world of Ex Marking [online]. URL: https://iecetech.org/issue/2017-04/The-hazardous-world-of-Ex-Marking. Accessed 15 February 2020.

23 Cisco Systems Inc. Networking and Security in Industrial Environments [online]. URL: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.pdf. Accessed February 2020.

24 American Institute of Chemical Engineers. Guidelines for Safe and Reliable Instrumented Protective Systems. Hoboken, NJ: Chichester: John Wiley & Sons Inc; 2007.

25 Risk Management Professionals Inc. SIL Verification [online]. URL: http://www.rmpcorp.com/sil/. Accessed 17 February 2020.

26 Lydon B. Automation.com. Multivendor Ethernet Safety Protocol – Noble Goal [online]. URL: https://www.automation.com/automation-news/article/multivendor-ethernet-safety-protocol-noble-goal. Accessed 25 February 2020.

27 EPSG. OpenSAFETY Protocol Specification [online]. URL: https://www.ethernet-powerlink.org/fileadmin/user_upload/Dokumente/Downloads/TECHNICAL_DOCUMENTS/EPSG_WDP_304_V-1-5-0__3_.pdf. Accessed 25 February 2020.

28 PI. PROFIsafe System Description [online]. URL: https://www.profibus.com/index.php?eID=dumpFile&t=f&f=51719&token=3ddb13f215c62bfc35ca8a5e4c4071e0c4bd006c. Accessed 1 March 2020.

29 PROFINET University. Industrial Safety: PROFIsafe Profile Overview [online]. URL: https://profinetuniversity.com/functional-safety/profisafe-profile-overview/. Accessed 1 March 2020.

30 Voss K. Control Engineering. CIP Safety: Fail-safe communication between nodes [online]. URL: https://www.controleng.com/articles/cip-safety-fail-safe-communication-between-nodes/. Accessed 3 March 2020.

31 EtherCAT Technology Group. Safety over EtherCAT Overview [online]. URL: https://www.ethercat.org/download/documents/Safety_over_EtherCAT_Overview.pdf. Accessed 3 March 2020.

32 Geng H. Internet of Things and Data Analytics Handbook. Hoboken, NJ: John Wiley & Sons Inc; 2017.

33 Gilchrist A. IoT Security Issues. Germany: DEG Press; 2017.

34 IIoT World. Four most hard to solve IIot security issues [online]. URL: https://iiot-world.com/cybersecurity/four-most-hard-to-solve-iiot-security-issues/. Accessed 14 March 2020.

35 Madhusanka L, Ahmad I, Abro A B, Gurtov A, Ylianttila M. A Comprehensive Guide to 5G Security. John Wiley & Sons Inc; 2018.

36 Siemens. Industrial Communication [online]. URL: https://new.siemens.com/global/en/products/automation/industrial-communication/5g.html. Accessed 14 March 2020.

37 Cisco. Time-Sensitive-Networking: A Technical Introduction [online]. URL: https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/white-paper-c11-738950.pdf

38 AL Presher, Industrial Ethernet Book, IEB media: Issue 113; 2019

39 Greenfield D. AutomationWorld. Industrial Ethernet: Safety over Ethernet [online]. URL: https://www.automationworld.com/products/control/blog/13311153/industrial-ethernet-safety-over-ethernet#previous-slide. Accessed 14 March 2020.

40 Cisco. Media Redundancy Protocol Configuration Guide for IE 2000, IE 4000, IE 4010, and IE 5000 Switches [online]. URL: https://www.cisco.com/c/en/us/td/docs/switches/connectedgrid/cg-switch-sw-master/software/configuration/guide/mrp/b_mrp_ie.html. Accessed 16 March 2020.

41 Hirschmann. PRP – Parallel Redundancy Protocol [online]. URL: https://hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/Technologies/PRP_-_Parallel_Redundancy_Protocol/index.phtml. Accessed 16 March 2020.

42 Hirschmann. HSR – High Availability Seamless Redundancy [online]. URL: https://hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/Technologies/HSR_uE2u80u93_High_Availability_Seamless_Redundancy/index.phtml. Accessed 16 March 2020.